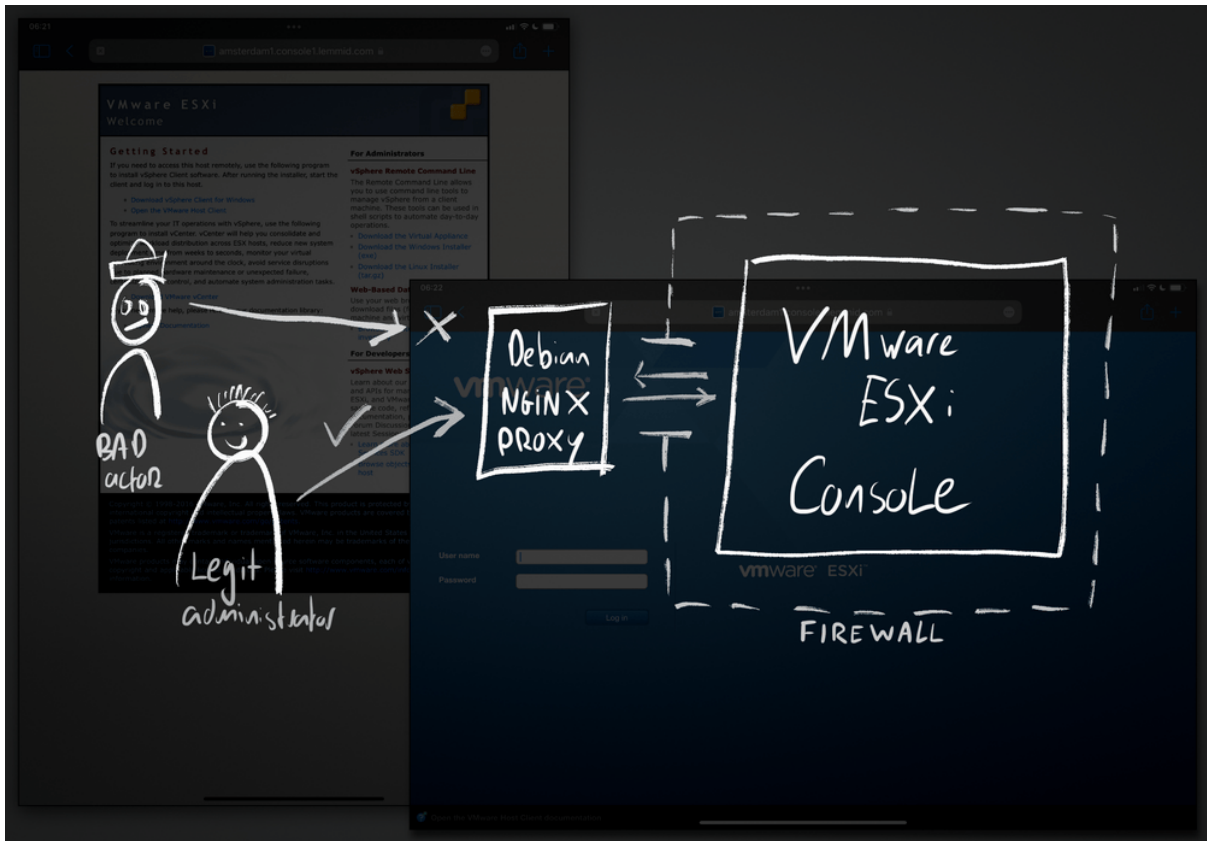


# VMware ESXi beveiligen

*Verbeter de beveiliging met een firewall en proxyserver*

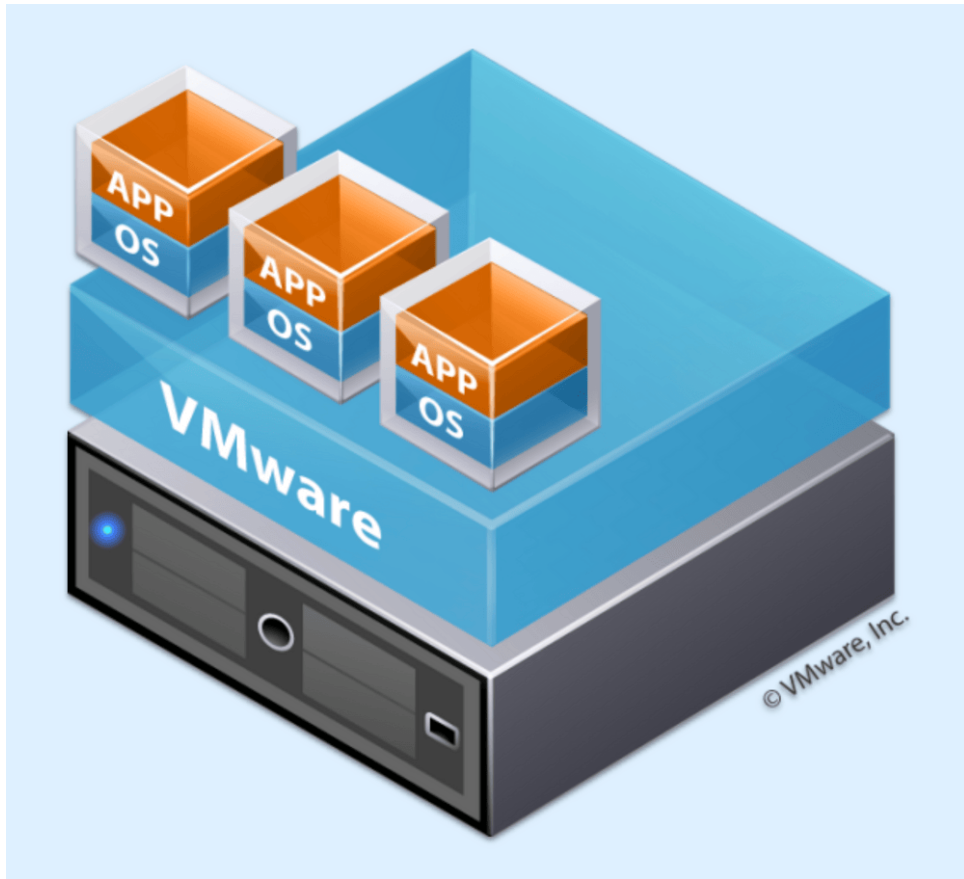
Willem L. Middelkoop

31 aug. 2021



Naar aanleiding van een incident op een server, heb ik een mogelijke inbreuk op de beveiliging gedetecteerd. De betreffende machine draaide VMware ESXi, een bare metal hypervisor die gebruikt wordt om virtuele privéservers te draaien. In standalone modus biedt een webgebaseerde beheerconsole volledige controle over de infrastructuur, wat een risico vormt.

Grote en krachtige serverhardware biedt een enorme reken capaciteit, vaak veel meer dan één applicatie nodig heeft. Door virtualisatie kunnen cloud operators het hardwaregebruik optimaliseren door dynamisch meerdere virtuele machines op één fysieke machine te laden.



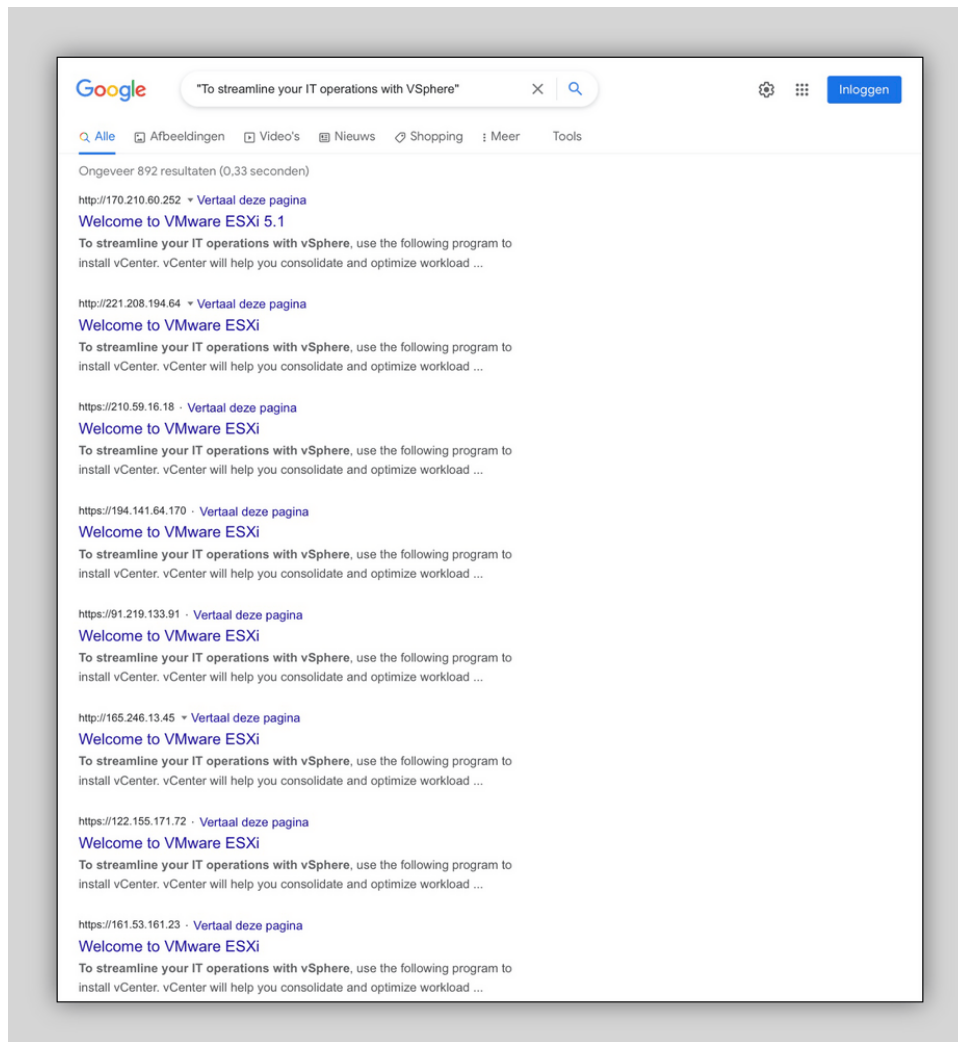
*VMware ESXi is een bare-metal hypervisor die één fysieke server opdeelt in meerdere virtuele servers*

Fysieke machines met VMware ESXi worden beheerd als gecentraliseerd vSphere-netwerk of als standalone machine. Beheerders maken, beheren en configureren virtuele machines via een krachtige webinterface. Zonder een gecentraliseerd vSphere-netwerk hebben beheerders deze webinterface nodig - maar deze openstellen op het publieke internet trekt ongewenste aandacht van hackers.



*VMware ESXi webinterface - waarmee jij en anderen deze fysieke machine kunnen beheren*

Kwaadwillende actoren zoeken actief naar blootgestelde beheerconsole's, in de hoop er een te vinden met een zwak wachtwoord of met bekende [security weaknesses](#). Laat de nieuwsgierige ontdekkingsreiziger in jezelf los en gebruik gewoon Google om [find a whole bunch of exposed machines with a special query](#). Zie mijn blogpost over [about special queries on Google](#) als je je zoekvaardigheden wilt opfrissen.

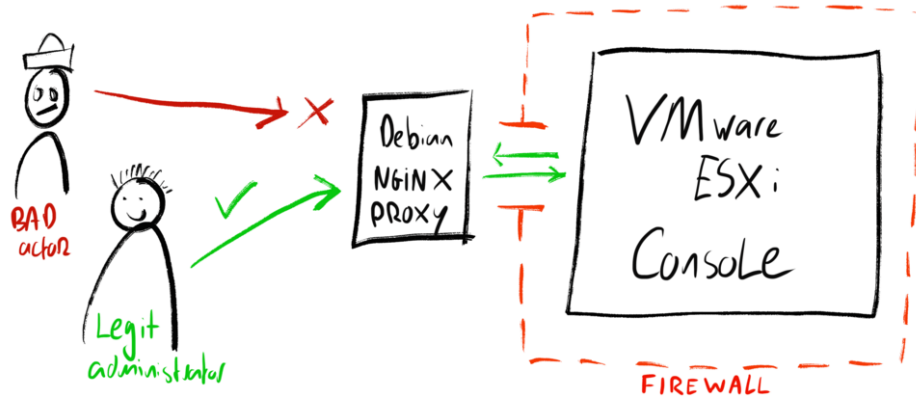


*Het vinden van blootgestelde VMware ESXi webinterfaces vereist niets meer dan wat Google-vaardigheden*

Laat de beheerconsole open en iedereen kan proberen in te loggen. Hackers en hun geautomatiseerde bots zullen dit zeker doen! Toegang op afstand voor lokale ESXi-gebruikersaccounts wordt tijdelijk geblokkeerd na meerdere mislukte inlogpogingen - voor iedereen! Dit kan frustrerend zijn wanneer jij als legitieme beheerder toegang tot de console nodig hebt.

Volgens mijn eigen [easy cyber security tips](#) kan de beveiliging van VMware ESXi worden verbeterd door de beheerconsole volledig te verbergen. Je zou in de verleiding kunnen komen om hiervoor een simpele "alles afdekkende" firewall te gebruiken, maar houd rekening met de noodzaak van de beheerconsole: deze biedt essentiële toegang tot actieve virtuele machines. Je wilt echt dat je beheerders 24/7 vanaf elke locatie toegang hebben tot de interface in geval van nood.

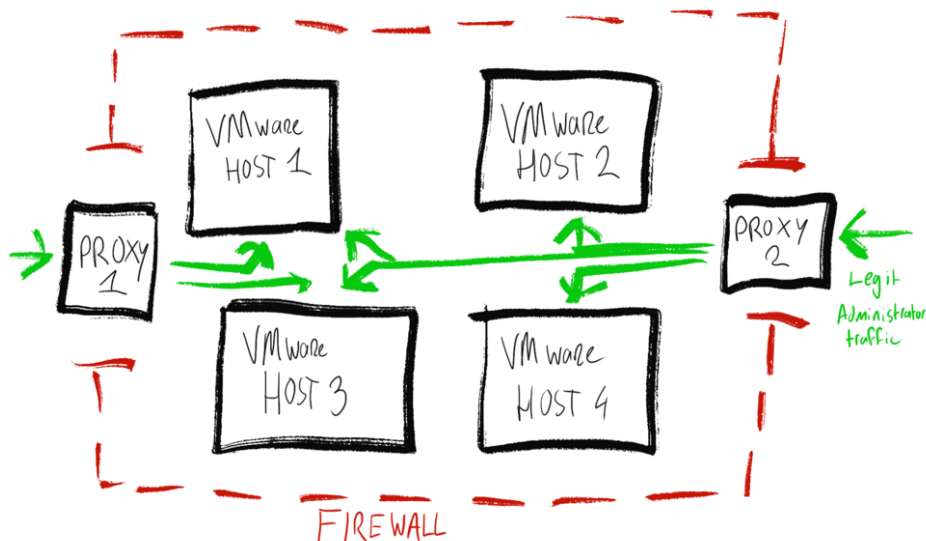
Dus in plaats van de beheerinterface volledig af te sluiten of te verbergen, zocht ik naar een manier om selectief toegang toe te staan, terwijl ik een onopvallend online profiel behield. Omdat ik wil dat legitieme beheerders vanaf elke locatie ter wereld toegang hebben tot de interface, kon ik geen simpel IP-adresfilter gebruiken. Met behulp van een Debian GNU/Linux-machine met nginx als proxyserver kan ik verkeer naar de beheerconsole vooraf authenticeren.



*Pre-authenticateer verkeer naar de beheerdersconsole via een kleine en eenvoudige Debian GNU/Linux-server met nginx-proxy*

In deze setup draait de Debian-machine op een apart netwerk, op andere hardware, met een vast IP-adres. De VMware-server accepteert alleen verkeer van deze proxyserver via zijn firewall. De proxyserver filtert verkeer met behulp van HTTP-authenticatie via SSL/TLS. Iedereen kan verbinding maken met de proxyserver, maar alleen degenen met geldige inloggegevens kunnen de VMWare-beheerconsole bereiken. De proxyserver lijkt een heel kleine, standaard webserver voor iedereen die hem scant: dit zorgt voor een onopvallende online signatuur.

Voeg nog een proxyserver van een ander netwerk op andere hardware toe aan de mix om een single point of failure te voorkomen. Nginx kan geauthenticeerd verkeer doorsturen naar verschillende beheerconsole's op basis van verschillende hostnamen, waardoor je één proxy kunt hergebruiken om meerdere VMware-machines te beveiligen. De proxy servers kunnen worden geconfigureerd om HTTP Basic-authenticatie te gebruiken met standaard en eenvoudige tools, bekijk de [nginx documentation for tips on this](#).



*Twee proxy servers die veilige toegang bieden tot meerdere VMware-hosts*

```

server {
    listen 80;
    server_name amsterdam1.console1.lemmid.com;

    root "/var/www/amsterdam1.console1.lemmid.com/";

    location /.well-known { }

    location / {
        return 301 https://amsterdam1.console1.lemmid.com$request_uri;
    }
}

server {
    listen 443 http2;
    listen [::]:443 http2;

    ssl on;
    ssl_certificate /etc/letsencrypt/live/amsterdam1.console1.lemmid.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/amsterdam1.console1.lemmid.com/privkey.pem;

    server_name amsterdam1.console1.lemmid.com;

    location / {
        auth_basic "Access is restricted" ;
        auth_basic_user_file /etc/console.lemmid.com.htpasswd;

        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $http_host;

        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-NginX-Proxy true;

        proxy_pass https://amsterdam1.lemmid.com;
        proxy_redirect off;
    }
}
~
"/etc/nginx/sites-available/amsterdam1.console1.lemmid.com" 42 lines, 1104 bytes

```

*nginx-configuratie om verkeer te authenticeren en door te sturen naar een VMware-beheerdersconsole*

## Conclusie

Door nginx als proxy voor de beheerconsole te gebruiken, kun je een authenticatielaag toevoegen *en* een onopvallende signatuur creëren voor iedereen die je netwerk scant. Dit verbetert de beveiliging van je VMware-machines door ze moeilijker te vinden en te benaderen te maken. Legitieme beheerders kunnen nog steeds toegang krijgen tot de beheerconsole met elke computer zonder de noodzaak van een VPN of vooraf geauthenticeerd IP-adres. Kwaadwillende actoren, hackers en bots zullen het moeilijk hebben om je te vinden. Je verstopt je in het volle zicht!